Authentifizierte Nessus-Tests für UNIX und Windows

17. Januar 2014

(Revision 32)

Inhaltsverzeichnis

Einleitung 4
Regeln und Konventionen 4
Übersicht über authentifizierte Nessus-Tests 4
Zweck 4
Ausmaß des Zugriffs 5
Verwendete Technologien 5
UNIX-Systeme 5
Benutzername und Kennwort 5
Öffentliche/private Schlüssel 6
Kerberos 6
Windows-Systeme 6
LanMan 6
NTLM und NTLMv2 6
SMB-Signierung 6
SPNEGO 7
Kerberos 7
NTLMSSP (NT Lan Manager Security Support Provider) und LMv2 7
Windows-Benutzernamen, Kennwörter und Domänen 7
Authentifizierte Tests auf UNIX-Plattformen 7
Voraussetzungen 7
Konfigurationsvoraussetzungen für SSH 7
Benutzerberechtigungen 8
Konfigurationsvoraussetzungen für Kerberos 8
Lokale Sicherheitstests mit SSH unter UNIX ermöglichen 8
Öffentlichen und privaten SSH-Schlüssel einrichten 8
Benutzerkonto erstellen und den SSH-Schlüssel einrichten 8
Beispiel 9
Nessus für hostbasierte SSH-Tests konfigurieren 10
Die Nessus-Benutzeroberfläche 10
Nessus-Befehlszeile für UNIX 13
.nessus-Dateien verwenden 14
.nessusrc-Dateien verwenden 14
SSH-Anmeldedaten mit Tenable SecurityCenter verwenden 14
Authentifizierte Tests auf Windows-Plattformen 15
Voraussetzungen 15
Benutzerberechtigungen 15
Windows-Anmeldenamen für lokale und Remoteaudits verwenden 15
Lokales Konto konfigurieren 15
Ein Domänenkonto für authentifizierte Scans konfigurieren 16
Schritt 1: Sicherheitsgruppe einrichten 16
Schritt 2: Gruppenrichtlinie einrichten 16
Schritt 3: Richtlinie konfigurieren, um die Gruppe „Nessus Local Access“ als Administratoren festzulegen 16
Schritt 4: Sicherstellen, dass die betreffenden Ports für die Nessus-Verbindung mit dem Host in der Firewall geöffnet sind 17
WMI über die Windows XP- und Windows 2003-Firewall zulassen 17
WMI über Windows Vista-, 7-, 8-, 2008-, 2008R2- und 2012-Firewall zulassen 18
Schritt 5: Gruppenrichtlinienobjekt verknüpfen 19
Windows XP und Windows 2003 konfigurieren 19

Windows 2008, Windows Vista und Windows 7 konfigurieren 19
Nessus für Windows-Anmeldungen konfigurieren 20
Die Nessus-Benutzeroberfläche 20
Nessus-Befehlszeile für UNIX 21
.nessus-Dateien verwenden 21
.nessusrc-Dateien verwenden 21
Fehlerhafte Anmeldedaten erkennen 21
Problembehebung 22
Wie Sie Ihren Scanner schützen 24
Warum sollte ich meinen Scanner schützen? 24
Wie schottet man einen Scanner ab? 24
Sichere Implementierung von SSH-Audits unter UNIX 24
Sichere Windows-Audits 24
Weitere Informationen 25
Wissenswertes zu Tenable Network Security 27

Einleitung

Das vorliegende Dokument beschreibt die Durchführung authentifizierter Netzwerkscans mit dem Sicherheitslückenscanner **Nessus** von Tenable Network Security. Authentifizierte Netzwerkscans ermöglichen das Abfragen „hostbasierter" Daten (z. B. fehlender Patches oder Betriebssystemeinstellungen) bei einem remote ausgeführten Netzwerkaudit. Wir freuen uns über Ihre Anmerkungen und Vorschläge. Senden Sie diese an support@tenable.com.

Nessus nutzt die Möglichkeit, sich über SSH (Secure Shell) bei UNIX-Remotehosts anzumelden. Für Windows-Hosts verwendet Nessus eine Vielzahl von Microsoft-Authentifizierungstechnologien.

Beachten Sie, dass Nessus auch das Simple Network Management Protocol (SNMP) zur Versions- und Datenabfrage bei Routern und Switches verwendet. Obwohl auch dies eine Form „lokaler" Tests ist, wird es nicht in diesem Dokument behandelt.

Während der Schwerpunkt in diesem Dokument in erster Linie auf Nessus liegt, gelten die beschriebenen Konzepte gleichermaßen für SecurityCenter von Tenable, auch wenn dies nicht ausdrücklich erwähnt ist.

Regeln und Konventionen

In der gesamten Dokumentation werden Dateinamen, Daemons und ausführbare Dateien in einer Schriftart wie **`courier bold`** angezeigt (z. B.: **`gunzip`**, **`httpd`** oder **`/etc/passwd`**).

Befehlszeilenoptionen und Schlüsselwörter werden ebenfalls in der Schriftart **`courier bold`** angezeigt. Die Befehlszeilen sind teils mit, teils ohne Befehlszeilen-Prompt und den Ausgabetext des betreffenden Befehls aufgeführt. In den Befehlszeilen erscheint der ausgeführte Befehl in der Schriftart **`courier bold`**, um zu verdeutlichen, was der Benutzer eingegeben hat. Die vom System generierte Beispielausgabe ist hingegen in der Schriftart `courier` (ohne Fettdruck) aufgeführt. Es folgt ein Beispiel für die Ausführung des UNIX-Befehls **`pwd`**:

```
# pwd
/home/test/
#
```

Wichtige Hinweise und Aspekte werden durch dieses Symbol und graue Textfelder hervorgehoben.

Tipps, Beispiele und Best Practices (Empfehlungen) werden durch dieses Symbol und weißen Text auf blauem Grund hervorgehoben.

Übersicht über authentifizierte Nessus-Tests

Nessus von Tenable ist ein sehr leistungsfähiger Sicherheitslückenscanner für das Netzwerk. Er bietet eine umfassende Datenbank aus Plugins, mit denen auf Vorhandensein einer Vielzahl von Sicherheitslücken geprüft werden kann, die remote nutzbar sind. Neben Remotescans kann Nessus auch zum Scannen lokaler Sicherheitslücken verwendet werden.

Zweck

Externes Scannen auf Sicherheitslücken im Netzwerk ist nützlich, um eine Momentaufnahme der im Netzwerk vorhandenen Dienste und der in ihnen möglicherweise vorhandenen Sicherheitslücken zu erstellen. Allerdings ist dies nur eine externe Perspektive. Es ist wichtig zu bestimmen, welche lokalen Dienste ausgeführt werden, und durch lokale Angriffe oder Konfigurationsfehler entstandene Sicherheitslücken zu erkennen, die das System für externe Angriffe anfällig machen könnten, aber bei einem externen Scan unter Umständen nicht erkannt werden.

Bei einer normalen Sicherheitslückenbewertung wird ein Remotescan für die externen Zugangspunkte und ein Onsite-Scan innerhalb des Netzwerks ausgeführt. Mit keinem dieser Scans lassen sich lokale Sicherheitslücken auf dem Zielsystem ermitteln. Ein Teil der erfassten Daten basiert auf den angezeigten Bannerinformationen, die möglicherweise

nicht aussagekräftig oder unzutreffend sind. Mithilfe sicherer Anmeldedaten kann dem Nessus-Scanner lokaler Zugriff auf dem Zielsystem gewährt werden, ohne dass hierfür ein Agent erforderlich ist. Dies ermöglicht das Scannen eines sehr großen Netzwerks zur Ermittlung lokaler Sicherheitslücken oder Complianceverstöße.

Das in Unternehmen am häufigsten zu findende Sicherheitsproblem ist, dass Sicherheitspatches nicht zeitnah aufgespielt werden. Durch einen authentifizierten Nessus-Scan kann schnell festgestellt werden, welche Systeme in Bezug auf die Patchinstallation nicht auf dem aktuellen Stand sind. Dies ist besonders wichtig, wenn eine neue Sicherheitslücke öffentlich gemacht wird und die Geschäftsleitung zeitnah über mögliche Auswirkungen auf die Organisation informiert werden möchte.

Ein weiterer wesentlicher Aspekt für Unternehmen ist die Compliance in Bezug auf Standortrichtlinien, Industriestandards (z. B. die CIS-Benchmarks des Center for Internet Security) oder Rechtsvorschriften wie Sarbanes-Oxley (SOX), Gramm-Leach-Bliley (GLBA) oder HIPAA. Organisationen, die Kreditkartendaten akzeptieren, müssen die Einhaltung der PCI-DSS-Standards (Payment Card Industry Data Security Standards) nachweisen. Es gibt eine ganze Reihe weithin bekannter Fälle, in denen Kreditkartendaten von Millionen von Kunden gestohlen wurden. Dies hat bei den Banken, die für die Deckung der Zahlungen zuständig waren, zu erheblichen finanziellen Einbußen geführt – und zu schweren Strafen oder dem Verlust der Kreditkartenakzeptanzfähigkeit bei den Händlern oder Verarbeitern, bei denen der Datendiebstahl erfolgte.

Ausmaß des Zugriffs

Authentifizierte Scans können alle Vorgänge ausführen, die auch einem lokalen Benutzer gestattet sind. Das Ausmaß des Zugriffs durch den Scan hängt von den Berechtigungen des Benutzerkontos ab, für das Nessus konfiguriert wurde.

Nichtberechtigte Benutzer mit lokalem Zugriff auf UNIX-Systeme können grundlegende Sicherheitsprobleme feststellen, z. B. im Zusammenhang mit Patchversionen oder Einträgen in die Datei **`/etc/passwd`**. Um jedoch umfassendere Informationen wie beispielsweise Systemkonfigurationsdaten oder systemweit gültige Dateiberechtigungen zu erhalten, ist ein Konto mit Root-Berechtigungen erforderlich.

Für authentifizierte Scans auf Windows-Systemen ist die Verwendung eines Administratorkontos notwendig. Verschiedene Bulletins und Softwareupdates von Microsoft haben dazu geführt, dass das Auslesen der Registrierung zur Ermittlung des Softwarepatchstandes ohne Administratorrechte unzuverlässig ist. Der Administratorzugriff ist erforderlich, um direkt aus dem Dateisystem lesen zu können. Auf diese Weise kann Nessus eine Verbindung mit einem Computer herstellen und mithilfe einer direkten Dateianalyse den tatsächlichen Patchstand des untersuchten Systems feststellen. Unter Windows XP Professional funktioniert dieser Dateizugriff mit einem lokalen Administratorkonto nur dann, wenn die Richtlinie „Netzwerkzugriff: Modell für gemeinsame Nutzung und Sicherheitsmodell für lokale Konten“ auf „Klassisch – lokale Benutzer authentifizieren sich als sie selbst“ umgestellt wurde.

Ein Audit zur SCAP-Compliance erfordert den Versand der ausführbaren Datei an den Remotehost. In Systemen, in denen Sicherheitssoftware (z. B. McAfee Host Intrusion Prevention) ausgeführt wird, wird die für das Audit erforderliche ausführbare Datei möglicherweise blockiert oder in Quarantäne versetzt. In diesem Fall muss eine Ausnahme wahlweise für den Host oder die versendete ausführbare Datei eingerichtet werden.

Verwendete Technologien

Die Herausforderung bei der Ausführung eines authentifizierten Scans besteht darin, die berechtigten Anmeldedaten auf sichere Weise an den Scanner zu übergeben. Der Zweck des Scannens zur Ermittlung von Sicherheitslücken würde gewiss verfehlt, wenn hierdurch eine noch größere Sicherheitslücke geöffnet würde. Nessus unterstützt die Verwendung verschiedener sicherer Methoden, um derartige Probleme auf UNIX- und Windows-Plattformen zu umgehen.

UNIX-Systeme

Auf UNIX-Systemen verwendet Nessus für hostbasierte Tests Programme, die auf dem SSH-Protokoll (Secure Shell) in Version 2 basieren (z. B. OpenSSH, Solaris SSH usw.). Solche Mechanismen verschlüsseln die Daten, um eine Erfassung durch Sniffer-Programme während der Übertragung zu verhindern. Nessus unterstützt drei Arten von Authentifizierungsmethoden zum Einsatz mit SSH: Benutzername und Kennwort, öffentliche/private Schlüssel und Kerberos.

Benutzername und Kennwort

Auch wenn die Möglichkeit zur SSH-Authentifizierung mit Benutzername und Kennwort vorhanden ist, rät Tenable von ihrer Verwendung ab. Vor allem dann, wenn sie bereits seit längerer Zeit verwendet werden, sind statische Kennwörter anfällig für Man-in-the-Middle- und Brute-Force-Angriffe.

Öffentliche/private Schlüssel
Die Verschlüsselung mit öffentlichen Schlüsseln – auch als Verschlüsselung mit asymmetrischen Schlüsseln bezeichnet – ist dank der Verwendung eines Schlüsselpaares aus öffentlichem und privatem Schlüssel eine sicherere Form der Authentifizierung. Bei der asymmetrischen Kryptographie wird der öffentliche Schlüssel zur Verschlüsselung von Daten und der private zu ihrer Entschlüsselung verwendet. Die Verwendung öffentlicher und privater Schlüssel ist eine Methode der SSH-Authentifizierung, die sich durch mehr Sicherheit und Flexibilität auszeichnet. Nessus unterstützt die Schlüsselformate DSA und RSA.

Kerberos
Das im Rahmen des Project Athena am Massachusetts Institute of Technology entwickelte Kerberos ist eine Client/Server-Anwendung, die ein Protokoll mit symmetrischer Verschlüsselung verwendet. Bei der symmetrischen Verschlüsselung wird zur Verschlüsselung von Daten und zu ihrer Entschlüsselung der gleiche Schlüssel verwendet. Unternehmen setzen ein KDC (Key Distribution Center, Schlüsselverteilcenter) ein, das alle Benutzer und Dienste enthält, die die Kerberos-Authentifizierung benötigen. Benutzer authentifizieren sich bei Kerberos, indem sie zunächst ein TGT (Ticket Granting Ticket, „ticketgewährendes“ Ticket) anfordern. Wird dem Benutzer ein TGT gewährt, so kann er dieses zur Anforderung von Diensttickets aus dem KDC verwenden und mit diesen andere Kerberos-basierte Dienste nutzen. Kerberos verwendet das CBC-(Cipher Block Chain-)DES-Verschlüsselungsprotokoll zur Verschlüsselung der gesamten Kommunikation.

Die Nessus-Implementierung der Kerberos-Authentifizierung für SSH unterstützt die Verschlüsselungsalgorithmen „aes-cbc“ und „aes-ctr“. Die Interaktion von Nessus mit Kerberos sieht im Überblick wie folgt aus:

- Der Endbenutzer gibt die IP-Adresse des KDC an.
- **`nessusd`** fragt bei **`sshd`** ab, ob die Kerberos-Authentifizierung unterstützt wird.
- **`sshd`** bejaht dies.
- **`nessusd`** fordert ein Kerberos-TGT nebst einem Anmeldenamen und einem Kennwort an.
- Kerberos schickt ein Ticket an **`nessusd`** zurück.
- **`nessusd`** gibt das Ticket an **`sshd`** weiter.
- **`nessusd`** ist angemeldet.

Windows-Systeme
Nessus unterstützt mehrere verschiedene Authentifizierungsmethoden für Windows-Systeme. Alle diese Methoden basieren auf der Verwendung eines Benutzernamens, eines Kennworts und eines Domänennamens (dieser ist in einigen Fällen für die Authentifizierung optional).

LanMan
Die LanMan-Authentifizierungsmethode war der wichtigste Ansatz unter Windows NT- und frühen Windows 2000-Serverbereitstellungen. Sie wird auf neueren Windows-Bereitstellungen eigentlich nicht mehr verwendet, wurde aber aus Gründen der Abwärtskompatibilität beibehalten.

NTLM und NTLMv2
Die mit Windows NT vorgestellte NTLM-Authentifizierungsmethode bietet im Vergleich zur LanMan-Authentifizierung mehr Sicherheit. Die erweiterte Version NTLMv2 ist in kryptografischer Hinsicht allerdings noch sicherer als NTLM und wird deswegen von Nessus standardmäßig zur Authentifizierung bei der Anmeldung an einem Windows-Server verwendet.

SMB-Signierung
Die SMB-Signierung ist eine kryptografische Prüfsumme, die auf den gesamten von einem Windows-Server empfangenen und gesendeten Datenverkehr angewendet wird. Viele Systemadministratoren aktivieren diese Funktion auf ihren Servern, um sicherzustellen, dass Remotebenutzer hundertprozentig authentifiziert und Mitglied einer Domäne werden. Sie wird von Nessus automatisch verwendet, sofern sie vom Windows-Remoteserver angefordert wird.

SPNEGO
Das SPNEGO-Protokoll (Simple and Protected Negotiate) bietet SSO-Funktionen (Single Sign On) für den Zugriff von einem Windows-Client auf eine Vielzahl geschützter Ressourcen unter Verwendung der Windows-Anmeldedaten des Benutzers. Nessus unterstützt die Verwendung von SPNEGO entweder mit NTLMSSP mit LMv2-Authentifizierung oder mit Kerberos und RC4-Verschlüsselung.

Kerberos
Nessus unterstützt die Verwendung der Kerberos-Authentifizierung auch in einer Windows-Domäne. Um sie zu konfigurieren, muss die IP-Adresse des Kerberos-Domänencontrollers (genauer gesagt: die IP-Adresse des Windows-Active Directory-Servers) angegeben werden.

NTLMSSP (NT Lan Manager Security Support Provider) und LMv2
Werden erweiterte Sicherheitssysteme wie Kerberos oder SPNEGO nicht unterstützt oder schlagen aus anderen Gründen fehl, dann probiert Nessus eine Anmeldung über die NTLMSSP/LMv2-Authentifizierung. Schlägt diese fehl, dann versucht Nessus eine Anmeldung unter Verwendung der NTLM-Authentifizierung.

Windows-Benutzernamen, Kennwörter und Domänen
Das SMB-Domänenfeld ist optional, und Nessus kann sich auch ohne dieses Feld unter Angabe der Domänenanmeldedaten anmelden. Benutzername, Kennwort und optionale Domänenangaben beziehen sich auf ein Konto, das dem Zielcomputer bekannt ist. Werden beispielsweise der Benutzername „joesmith“ und das Kennwort „`my4x4mpl3`“ angegeben, dann sucht der Windows-Server diesen Benutzernamen zunächst aus der Liste der Benutzer auf dem lokalen System heraus und bestimmt dann, ob er dort auch Teil einer Domäne ist.

Der tatsächliche Domänenname ist nur erforderlich, wenn der Kontennamen in der Domäne von dem auf dem Computer abweicht. Es ist uneingeschränkt möglich, ein Konto namens „Administrator“ sowohl auf einem Windows-Server als auch in der Domäne zu verwenden. In diesem Fall wird zur Anmeldung auf dem lokalen Server der Benutzername „Administrator“ mit dem Kennwort des betreffenden Kontos verwendet. Auch zur Anmeldung an der Domäne würde der Benutzername „Administrator“ benutzt, diesmal allerdings mit dem Domänenkennwort und unter Angabe des Domänennamens.

Unabhängig von den verwendeten Anmeldedaten versucht Nessus stets, sich mit den folgenden Kombinationen an einem Windows-Server anzumelden:

- „Administrator“ ohne Kennwort
- Zufällig gewählte Angaben zu Benutzername und Kennwort, um Gästekonten zu testen
- Keine Angabe für Benutzername und Kennwort, um Nullsitzungen zu testen

Authentifizierte Tests auf UNIX-Plattformen

Der in diesem Abschnitt beschriebene Vorgang ermöglicht es Ihnen, lokale Sicherheitstests auf UNIX-Systemen (z. B. Linux, Solaris oder Mac OS X) auszuführen. Der in diesem Beispiel verwendete SSH-Daemon ist OpenSSH. Bei Verwendung einer kommerziellen SSH-Variante kann sich der Vorgang geringfügig anders gestalten.

Zum Ermöglichen lokaler Sicherheitstests lassen sich zwei grundlegende Methoden verwenden:

1. Verwendung eines SSH-Schlüsselpaars aus privatem und öffentlichem Schlüssel
2. Benutzeranmeldedaten und **`sudo`**-Zugriff, oder Anmeldedaten für den **`su`**-Zugriff

Voraussetzungen

Konfigurationsvoraussetzungen für SSH

Nessus 5 unterstützt die folgenden Algorithmen: blowfish-cbc, aesXXX-cbc (aes128, aes192 und aes256), 3des-cbc und aes-ctr.

Der Blowfish-Algorithmus wird – vermutlich aufgrund von Exportfragen – von einigen kommerziellen SSH-Varianten nicht unterstützt. Ein SSH-Server kann auch so konfiguriert werden, dass er nur bestimmte Verschlüsselungstypen akzeptiert. Stellen Sie sicher, dass der erforderliche Algorithmus auf Ihrem SSH-Server unterstützt wird.

Benutzerberechtigungen

Für eine optimale Leistung muss der SSH-Benutzer die Möglichkeit haben, jeden beliebigen Befehl auf dem System auszuführen. Auf UNIX-Systemen spricht man hierbei von „**root**-Berechtigungen“. Zwar lassen sich einige Tests (etwa auf Patchversionen) auch mit eingeschränkten Rechten ausführen, doch ist für die vollständigen Compliancetests, bei denen die Systemkonfigurationen und die Dateiberechtigungen überprüft werden, Root-Zugriff erforderlich. Aus diesem Grund wird dringend empfohlen, SSH-Schlüssel anstelle von Anmeldedaten zu verwenden.

Konfigurationsvoraussetzungen für Kerberos

Wenn Kerberos verwendet wird, muss **sshd** mit Kerberos-Unterstützung konfiguriert werden, damit das vom KDC erhaltene Ticket verifiziert werden kann. Damit dies funktioniert, müssen Reverse-DNS-Lookups korrekt konfiguriert worden sein. Als Kerberos-Interaktionsmethode muss **gssapi-with-mic** festgelegt sein.

Lokale Sicherheitstests mit SSH unter UNIX ermöglichen

Dieser Abschnitt vermittelt einen Überblick über die Aktivierung von SSH zwischen den an authentifizierten Nessus-Tests beteiligten Systemen. Er ist nicht als umfassende Einführung in SSH gedacht. Es wird vorausgesetzt, dass der Leser über die erforderlichen Kenntnisse im Bereich der UNIX-Systembefehle verfügt.

Öffentlichen und privaten SSH-Schlüssel einrichten

Der erste Schritt besteht in der Einrichtung eines Schlüsselpaares aus öffentlichem und privatem Schlüssel, das vom Nessus-Scanner eingesetzt werden kann. Dieses Schlüsselpaar kann auf einem beliebigen UNIX-System und unter Verwendung eines beliebigen Benutzerkontos erstellt werden. Allerdings ist es wichtig, dass der definierte Nessus-Benutzer Besitzer der Schlüssel ist.

Verwenden Sie zur Generierung des Schlüsselpaares **ssh-keygen**. Speichern Sie den Schlüssel danach an einem sicheren Ort. Im folgenden Beispiel werden die Schlüssel auf einer Red Hat-ES 3-Installation erstellt.

```
# ssh-keygen -t dsa
Generating public/private dsa key pair.
Enter file in which to save the key (/Users/test/.ssh/id_dsa):
       /home/test/Nessus/ssh_key
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in
/home/test/Nessus/ssh_key.
Your public key has been saved in
/home/test/Nessus/ssh_key.pub.
The key fingerprint is:
06:4a:fd:76:ee:0f:d4:e6:4b:74:84:9a:99:e6:12:ea
#
```

Übertragen Sie den privaten Schlüssel ausschließlich auf das System, auf dem der Nessus-Server ausgeführt wird, aber nicht an andere Systeme. Wenn **ssh-keygen** zur Eingabe einer Passphrase auffordert, geben Sie eine starke Passphrase ein oder drücken Sie zweimal auf die Eingabetaste (in diesem Fall wird durch keine Passphrase festgelegt). Wenn eine Passphrase angegeben wird, muss die Angabe unter „Policies“ („Richtlinien“) > „Credentials“ („Berechtigungen“) > „SSH Settings Options“ („SSH-Einstellungsoptionen“) erfolgen, damit Nessus die schlüsselbasierte Authentifizierung verwenden kann.

Benutzer von Nessus für Windows sollten auf dem System, auf dem Nessus ausgeführt wird, beide Schlüssel in das Anwendungshauptverzeichnis von Nessus (standardmäßig **C:\Programme\Tenable\Nessus**) kopieren. Den öffentlichen Schlüssel kopieren Sie dann nach Bedarf auf die Zielsysteme. Dies erleichtert die Verwaltung privater und öffentlicher Schlüsseldateien.

Benutzerkonto erstellen und den SSH-Schlüssel einrichten

Erstellen Sie auf jedem Zielsystem, das unter Verwendung eines lokalen Sicherheitstests gescannt werden soll, ein neues Benutzerkonto, das der Verwendung durch Nessus vorbehalten ist. Dieses Benutzerkonto muss auf allen Systemen exakt

den gleichen Namen haben. Im Folgenden haben wir diesen Benutzer „nessus“ genannt, Sie können aber jeden beliebigen anderen Namen verwenden.

Nach der Erstellung des Kontos für den Benutzer stellen Sie sicher, dass für dieses Konto kein gültiges Kennwort festgelegt wurde. Auf Linux-Systemen werden neue Benutzerkonten standardmäßig gesperrt, sofern nicht ausdrücklich zu Beginn ein Kennwort festgelegt wurde. Wenn Sie ein Konto verwenden, für das ein Kennwort festgelegt wurde, sperren Sie das Konto mit dem Befehl „**`passwd -l`**“.

Außerdem müssen Sie im Stammverzeichnis dieses neuen Kontos ein Unterverzeichnis erstellen, das den öffentlichen Schlüssel enthält. Im Folgenden verwenden wir hierfür das Verzeichnis **`/home/nessus/.ssh`**. Nachfolgend gezeigt ist ein Beispiel für Linux-Systeme:

```
# passwd -l nessus
# cd /home/nessus
# mkdir .ssh
#
```

Bei Solaris 10-Systemen hat Sun den Befehl „**`passwd(1)`**“ so erweitert, dass zwischen gesperrten und Nichtanmeldekonten unterschieden wird. Hierdurch soll sichergestellt werden, dass ein gesperrtes Benutzerkonto nicht zur Ausführung von Befehlen (z. B. Cron-Jobs) verwendet werden kann. Nichtanmeldekonten werden nur zur Ausführung von Befehlen, nicht aber zur Unterstützung einer interaktiven Anmeldesitzung verwendet. Bei solchen Konten steht das Kürzel „NP“ im Kennwortfeld von **`/etc/shadow`**. Führen Sie zur Festlegung eines Nichtanmeldekontos und zur Erstellung des Verzeichnisses für den öffentlichen SSH-Schlüssel in Solaris 10 die folgenden Befehle aus:

```
# passwd -N nessus

# grep nessus /etc/shadow
nessus:NP:13579::::::
# cd /export/home/nessus
# mkdir .ssh
#
```

Nach der Erstellung des Benutzerkontos müssen Sie den Schlüssel auf das System übertragen, ihn im passenden Verzeichnis ablegen und die richtigen Berechtigungen festlegen.

Beispiel

Kopieren Sie wie nachfolgend gezeigt den öffentlichen Schlüssel von dem System, auf dem die Schlüssel gespeichert sind, auf das System, das auf Hosttests gescannt wird. 192.1.1.44 ist ein Beispiel für ein Remotesystem, das mit hostbasierten Tests getestet wird.

```
# scp ssh_key.pub root@192.1.1.44:/home/nessus/.ssh/authorized_keys
#
```

Sie können die Datei auch von dem System kopieren, auf dem Nessus installiert ist. Hierzu verwenden Sie den Secure FTP-Befehl „**`sftp`**“. Beachten Sie, dass die Datei auf dem Zielsystem den Namen „authorized_keys“ tragen muss.

Kehren Sie wieder zum System zurück, auf dem der öffentliche Schlüssel abgelegt ist.

Legen Sie die Berechtigungen sowohl für das Verzeichnis **`/home/nessus/.ssh`** als auch für die Datei **`authorized_keys`** fest.

```
# chown -R nessus:nessus ~nessus/.ssh/
# chmod 0600 ~nessus/.ssh/authorized_keys
```

```
# chmod 0700 ~nessus/.ssh/
#
```

Wiederholen Sie diesen Vorgang – beginnend beim obigen Abschnitt „Benutzerkonto erstellen und den SSH-Schlüssel einrichten“ – auf allen Systemen, die für SSH-Tests überprüft werden sollen.

Führen Sie Tests durch, um sicherzustellen, dass die Konten und Netzwerke korrekt konfiguriert sind. Führen Sie unter Verwendung des einfachen UNIX-Befehls „**id**“ vom Nessus-Scanner aus den folgenden Befehl aus:

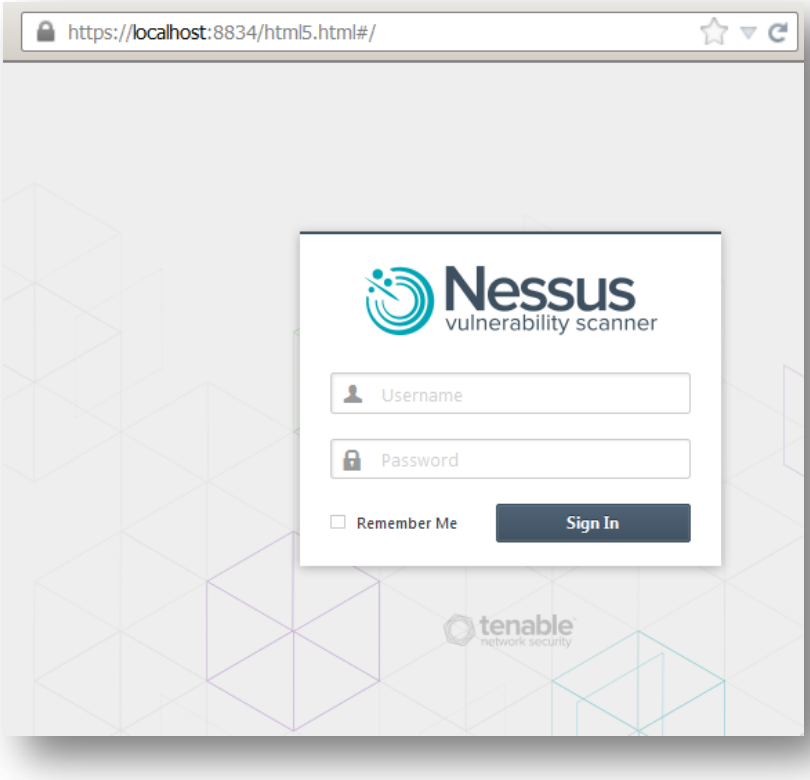
```
# ssh -i /home/test/nessus/ssh_key nessus@192.1.1.44 id
uid=252(nessus) gid=250(tns) groups=250(tns)
#
```

Werden Informationen zum Benutzer „nessus“ zurückgegeben, dann war der Schlüsselaustausch erfolgreich.

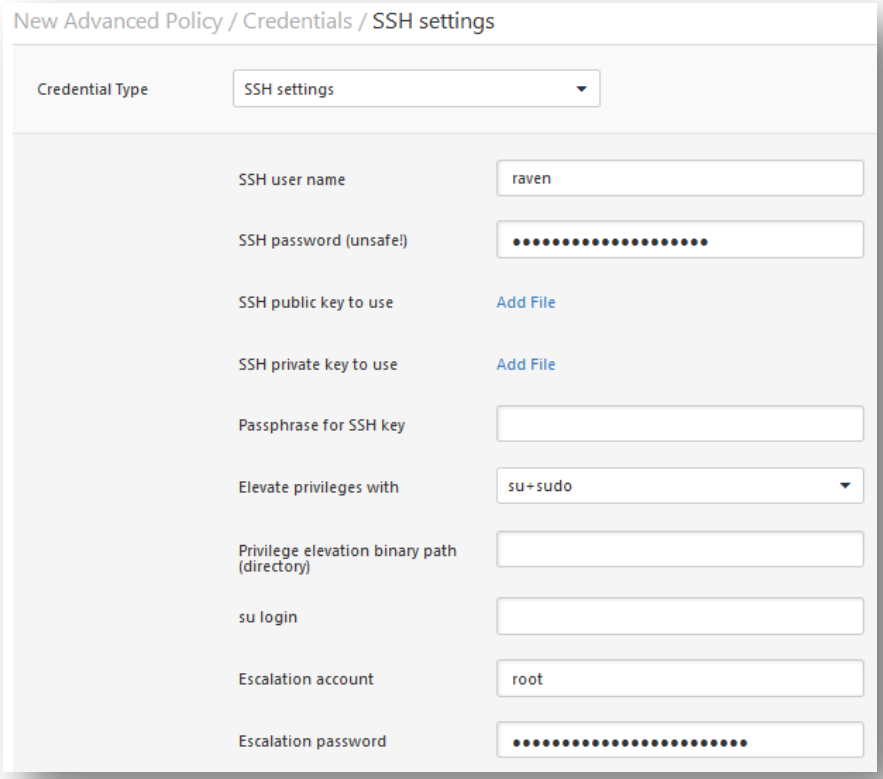
Nessus für hostbasierte SSH-Tests konfigurieren

Die Nessus-Benutzeroberfläche

Sofern Sie dies nicht bereits getan haben, kopieren Sie die private und die öffentliche Schlüsseldatei auf sicherem Wege auf das System, das Sie für den Zugriff auf den Nessus-Scanner verwenden werden.



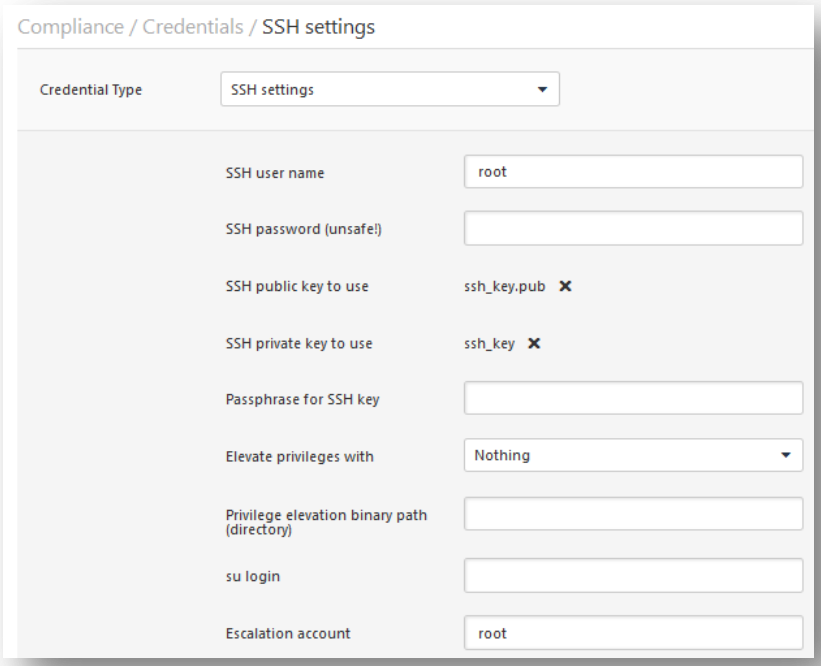
Öffnen Sie einen Webbrowser, stellen Sie wie oben gezeigt eine Verbindung mit der Benutzeroberfläche des Nessus-Scanners her und klicken Sie auf die Registerkarte „Policies“ („Richtlinien“). Erstellen Sie eine neue oder bearbeiten Sie eine vorhandene Richtlinie und wählen Sie dann die Registerkarte „Credentials“ („Anmeldedaten“) auf der linken Seite aus. Wählen Sie „SSH settings“ („SSH-Einstellungen“) aus dem Dropdownmenü oben im Fenster aus:



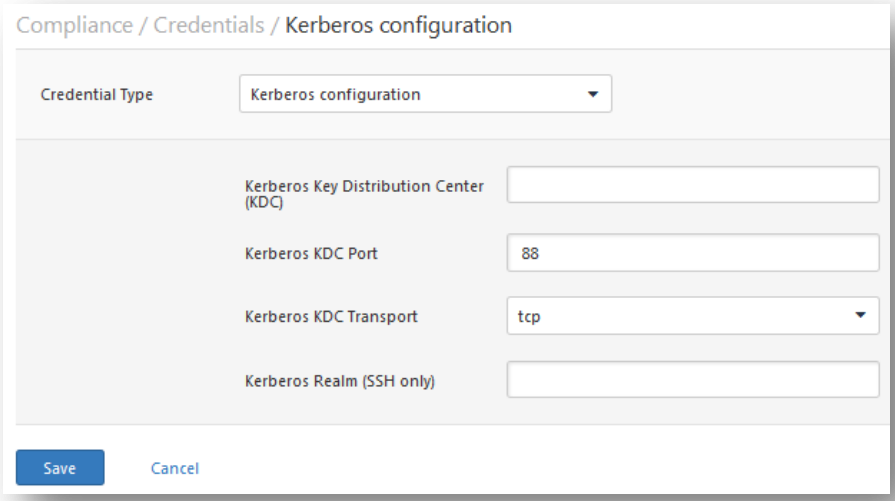
- Geben Sie auf allen Zielsystemen für das Element „SSH user name“ („SSH-Benutzername“) den Namen des für Nessus vorgesehenen Kontos ein. Standardmäßig ist der Eintrag auf „root“ festgelegt.
- Wenn Sie ein Kennwort für SSH verwenden, geben Sie es in das Feld „SSH password“ („SSH-Kennwort“) ein.
- Verwenden Sie wie empfohlen SSH-Schlüssel anstelle eines Kennworts, dann klicken Sie auf die Schaltfläche „Select“ („Auswählen“) neben dem Feld „SSH public key to use“ („Zu verwendender öffentlicher SSH-Schlüssel“) und navigieren Sie zur öffentlichen Schlüsseldatei auf dem lokalen System.
- Klicken Sie für das Element „SSH private key to use“ („Zu verwendender privater SSH-Schlüssel“) auf die Schaltfläche „Select“ und navigieren dann zu derjenigen privaten Schlüsseldatei auf dem lokalen System, die zu dem oben gewählten öffentlichen Schlüssel gehört.
- Wenn Sie eine Passphrase für SSH verwenden (optional), geben Sie sie in das Feld „Passphrase for SSH key“ („Passphrase für SSH-Schlüssel“) ein.
- Nessus- und SecurityCenter-Benutzer können mit dem Feld „Elevate privileges with“ („Berechtigungen hochstufen mit“) und einem separaten Kennwort „**`su`**“ oder „**`sudo`**“ aufrufen.
- Wenn die SSH-Datei „**`known_hosts`**“ vorhanden und als Teil der Scanrichtlinie im Feld „SSH known_hosts file“ („SSH-Datei 'known_hosts'“) angegeben ist, wird Nessus sich, sofern möglich, nur bei den in dieser Datei genannten Hosts anmelden. Auf diese Weise kann sichergestellt werden, dass derselbe Benutzername und dasselbe Kennwort, die Sie für Audits Ihrer bekannten SSH-Server verwenden, nicht zur Anmeldung auf einem System verwendet wird, das sich nicht unter Ihrer Kontrolle befindet.

Die wirksamsten authentifizierten Scans sind solche, bei denen das angegebene Konto über Root-Berechtigungen verfügt. Da zahlreiche Sites eine Remoteanmeldung als Root nicht zulassen, können Nessus-Benutzer „**`su`**“ oder „**`sudo`**“ mit einem separaten Kennwort für ein Konto aufrufen, für das „**`su`**“- oder „**`sudo`**“-Berechtigungen konfiguriert wurden.

Es folgt ein Screenshot der Verwendung von „**`sudo`**“ in Verbindung mit SSH-Schlüsseln. In diesem Beispiel heißt das Benutzerkonto „audit“ und wurde der Datei **`/etc/sudoers`** auf dem zu scannenden System hinzugefügt. Angegeben wird das Kennwort für das Konto „audit“, nicht das Root-Kennwort. Die SSH-Schlüssel entsprechen Schlüsseln, die für das Konto „audit“ erstellt wurden:



Wenn Sie Kerberos verwenden, müssen Sie einen Nessus-Scanner so konfigurieren, dass er sich bei einem KDC authentifiziert. Wählen Sie „Kerberos configuration“ („Kerberos-Konfiguration“) wie nachfolgend gezeigt aus dem Dropdownmenü aus:



Der KDC-Standardport ist „88“, und das Standardtransportprotokoll ist „udp“. Der andere mögliche Wert für das Transportprotokoll ist „tcp“. Schließlich sind noch der Kerberos-Bereichsname („Kerberos Realm“) und die IP-Adresse des KDC erforderlich.

Beachten Sie, dass Sie, um diese Authentifizierungsmethode verwenden zu können, bereits eine Kerberos-Umgebung eingerichtet haben müssen.

Klicken Sie nun unten im Fenster auf „**Submit**“ („Absenden“), um die Konfiguration abzuschließen. Die neue Scanrichtlinie wird nun der Liste der verwalteten Scanrichtlinien hinzugefügt.

Nessus-Befehlszeile für UNIX

Die Nessus-Unterstützung für hostbasierte Tests ist ab Nessus 2.2.0 verfügbar und erfordert die Einkompilierung der SSL-Unterstützung. Führen Sie den Befehl „**`nessusd -d`**“ aus, um zu überprüfen, ob Ihre Version und die SSL-Bibliotheken korrekt sind:

```
# nessusd -d
[root@squirrel sbin]# ./nessusd -d
This is Nessus 5.0.1. [build R23100] for Linux 2.6.18-53.1.6.el5
compiled with gcc version 4.1.2 20070626 (Red Hat 4.1.2-14)
Current setup :
       flavor                          : es5-x86
       nasl                            : 5.0.1
       libnessus                       : 5.0.1
       SSL support                     : enabled
       SSL is used for client / server communication
       Running as euid                 : 0
Magic hash: 49edd1433ffad7b87b446a4201faeedf -
OpenSSL: OpenSSL 1.0.0g 18 Jan 2012
```

.nessus-Dateien verwenden
Nessus kann konfigurierte Scanrichtlinien, Netzwerkziele und Berichte als **.nessus**-Datei speichern. Die Erstellung einer **.nessus**-Datei, die SSH-Anmeldedaten enthält, ist weiter oben im Abschnitt „Die Nessus-Benutzeroberfläche“ beschrieben. Hinweise zur Ausführung eines Befehlszeilenscans mithilfe der **.nessus**-Datei entnehmen Sie dem Nessus-Benutzerhandbuch. Dieses ist verfügbar unter:

http://www.tenable.com/products/nessus/documentation

.nessusrc-Dateien verwenden
Wenn Sie **.nessusrc**-Dateien manuell erstellen, können Sie mehrere Parameter zur Angabe der SSH-Authentifizierung konfigurieren. Nachfolgend gezeigt ist ein Beispiel eines nicht gefüllten Listings:

```
Use SSH to perform local security checks[entry]:SSH user name : =
Use SSH to perform local security checks[file]:SSH public key to use : =
Use SSH to perform local security checks[file]:SSH private key to use : =
Use SSH to perform local security checks[password]:Passphrase for SSH key : =
SSH settings[entry]:SSH user name : =
SSH settings[password]:SSH password (unsafe!) : =
SSH settings[file]:SSH public key to use : = no
SSH settings[file]:SSH private key to use : =
SSH settings[password]:Passphrase for SSH key : =
```

Wenn Sie Kerberos verwenden, müssen Sie einen Nessus-Scanner so konfigurieren, dass er sich bei einem KDC authentifiziert. Hierzu geben Sie die folgenden Informationen in die **nessusrc**-Datei des Scanners ein:

```
Kerberos KDC port : 88
Kerberos KDC Transport : udp
Kerberos Realm (SSH Only) : myrealm
Kerberos Key Distribution Center (KDC): 192.168.20.66
```

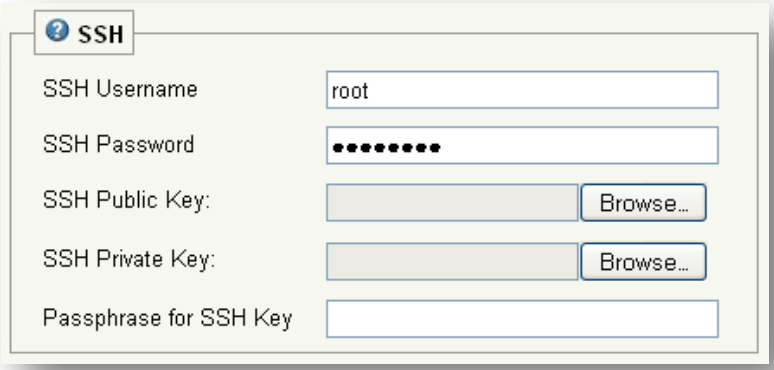
Der KDC-Standardport ist „88“, und das Standardtransportprotokoll ist „udp“. Der andere mögliche Wert für das Transportprotokoll ist „tcp“. Schließlich sind noch der Kerberos-Bereichsname („Kerberos Realm“) und die IP-Adresse des KDC erforderlich.

Beachten Sie, dass Sie, um diese Authentifizierungsmethode verwenden zu können, bereits eine Kerberos-Umgebung eingerichtet haben müssen.

SSH-Anmeldedaten mit Tenable SecurityCenter verwenden

Laden Sie zur Verwendung der SSH-Anmeldedaten mit SecurityCenter die erstellten öffentlichen und privaten SSH-Schlüssel in die SecurityCenter-Konsole hoch. Installieren Sie sie nicht direkt auf den Nessus-Scanner, weil SecurityCenter diese Anmeldedaten in den Nessus-Scanner lädt, wenn der Scan eingeleitet wird.

Nachfolgend gezeigt ist ein Beispiel des Fensterbereichs „Edit Scan Options“ („Scanoptionen bearbeiten“) beim Bearbeiten der Optionen einer Richtlinie. In den letzten drei Feldern sind ein Konto und die erforderlichen öffentlichen und privaten SSH-Schlüssel angegeben, die für die Tests verwendet werden. Der öffentliche SSH-Schlüssel muss auf jeden UNIX-Host gespeichert werden, der auf diese Weise „lokal“ getestet wird.



SecurityCenter umfasst bei der Auslieferung bereits eine Anzahl vordefinierter Richtlinien zu Sicherheitslücken, bei denen alle „lokalen“ Tests für die jeweiligen Betriebssysteme aktiviert sind. Um diese Richtlinien jedoch verwenden zu können, müssen sie zunächst kopiert werden, und es müssen ihnen ein bestimmtes SSH-Schlüsselpaar sowie ein bestimmtes Benutzerkonto hinzugefügt werden.

Die SSH-Schlüsselpaare werden von SecurityCenter verwaltet und an jeden verwalteten Nessus-Scanner übergeben.

Sobald die öffentlichen SSH-Schlüssel auf den gewünschten UNIX-Hosts und die privaten Schlüssel unter SecurityCenter installiert wurden, wird eine Vertrauensbeziehung hergestellt, die es Benutzern gestattet, sich von den Nessus-Scannern aus an jedem UNIX-Host anzumelden. Besteht die Gefahr, dass die Nessus-Scanner nicht mehr sicher sind, dann müssen neue öffentliche und private SSH-Schlüssel generiert werden.

Authentifizierte Tests auf Windows-Plattformen

Voraussetzungen

Benutzerberechtigungen

Ein Fehler, der sehr häufig gemacht wird, besteht darin, ein lokales Konto zu erstellen, das nicht über ausreichende Berechtigungen verfügt, um eine Remoteanmeldung durchzuführen und sinnvolle Maßnahmen zu ergreifen. Standardmäßig erhalten neue lokale Konten unter Windows Gastberechtigungen, sofern die Anmeldung remote erfolgte. Hierdurch werden remote ausgeführte Sicherheitslückenaudits unmöglich gemacht. Ein weiterer häufiger Fehler ist die Erweiterung des Zugriffs, den Gastbenutzer erhalten können. Dies verringert die Sicherheit Ihres Windows-Servers.

Windows-Anmeldenamen für lokale und Remoteaudits verwenden

Der wichtigste Aspekt im Zusammenhang mit Windows-Anmeldedaten besteht darin, dass das Konto, das zur Durchführung der Tests verwendet wird, über Berechtigungen für den Zugriff auf alle erforderlichen Dateien und Registrierungseinträge verfügen muss. In vielen Fällen ist dies gleichbedeutend mit Administratorrechten. Wenn Nessus nicht über die Anmeldedaten eines Administratorkontos verfügt, kann es maximal verwendet werden, um in der Registrierung Informationen zu Patches zu ermitteln. Dies ist zwar auch eine zulässige Methode, um festzustellen, ob ein Patch installiert ist, aber inkompatibel mit einigen Patchverwaltungstools von Drittanbietern, die es unter Umständen versäumen, den Schlüssel in der Richtlinie festzulegen. Wenn Nessus über Administratorrechte verfügt, wird die Version der `.dll`-Datei (Dynamic Link Library) auf dem Remotehost direkt überprüft, was wesentlich genauer ist.

Lokales Konto konfigurieren

Um einen Windows-Server, der nicht zu einer Domäne gehört, mit Anmeldedaten zu konfigurieren, müssen Sie lediglich ein eindeutiges Konto als Administrator erstellen.

Stellen Sie sicher, dass die Konfiguration dieses Kontos nicht den üblichen Vorgabewert „Nur Gast – lokale Benutzer authentifizieren sich als Gast“ verwendet. Ändern Sie diesen stattdessen in „Klassisch – lokale Benutzer authentifizieren sich als sie selbst“.

Um den Server so zu konfigurieren, dass er Anmeldungen über ein Domänenkonto zulässt, muss das Sicherheitsmodell „Klassisch“ aufgerufen werden. Gehen Sie zu diesem Zweck wie folgt vor:

1. Öffnen Sie „Gruppenrichtlinie“, indem Sie auf „Start“ > „Ausführen“ klicken, „**`gpedit.msc`**“ eingeben und abschließend auf „OK“ klicken.

2. Wählen Sie „Computerkonfiguration“ > „Windows-Einstellungen“ > „Sicherheitseinstellungen“ > „Lokale Richtlinien“ > „Sicherheitsoptionen“ aus.

3. Öffnen Sie in der Liste die Richtlinie „Netzwerkzugriff: Modell zur gemeinsamen Nutzung und Sicherheitsmodell für lokale Konten“.

4. Wählen Sie in diesem Dialog „Klassisch - lokale Benutzer authentifizieren sich als sie selbst“ aus und klicken Sie auf „OK“, um die Auswahl zu speichern.

Dies hat zur Folge, dass lokale Domänenbenutzer sich als sich selbst authentifizieren, auch wenn sie für den betreffenden Server eigentlich nicht „lokal“ im engeren Sinne sind. Ohne diesen Schritt müssten sich alle Remotebenutzer – einschließlich der echten Benutzer in der Domäne – als „Gast“ authentifizieren und würden in diesem Fall nicht über ausreichende Rechte zur Durchführung eines Remote-Audits verfügen.

Beachten Sie, dass das Tool **`gpedit.msc`** in einigen Versionen wie dem von Tenable nicht unterstützten Windows 7 Home nicht verfügbar ist.

Ein Domänenkonto für authentifizierte Scans konfigurieren

Zur Erstellung eines Domänenkontos für hostbasierte Remote-Audits auf einem Windows-Server muss der Server unter einem der Betriebssysteme Windows Vista, Windows XP Professional, Windows 2003, Windows 2008, Windows 7 oder Windows 8 ausgeführt werden und zudem Teil einer Domäne sein. Es sollten unter Berücksichtigung der Sicherheit fünf allgemeine Schritte zur Einrichtung dieses Scans erfolgen.

Schritt 1: Sicherheitsgruppe einrichten
Richten Sie zunächst eine Sicherheitsgruppe namens **Nessus Local Access** ein:

- Melden Sie sich beim Domänencontroller an und öffnen Sie „Active Directory-Benutzer und -Computer“.

- Erstellen Sie die Sicherheitsgruppe im Menü. Wählen Sie dazu **Aktion** > **Neu** > **Gruppe** aus.

- Nennen Sie die Gruppe **Nessus Local Access**. Achten Sie darauf, dass als Bereich `Global` und als Typ `Sicherheit` festgelegt sind.

- Fügen Sie der Gruppe **Nessus Local Access** das Konto hinzu, das Sie zur Ausführung von authentifizierten Nessus-Scans unter Windows verwenden werden.

Schritt 2: Gruppenrichtlinie einrichten
Als Nächstes müssen Sie eine Gruppenrichtlinie namens **Local Admin GPO** einrichten.

- Öffnen Sie die **Gruppenrichtlinien-Verwaltungskonsole**.

- Klicken Sie mit der rechten Maustaste auf **Gruppenrichtlinienobjekte** und wählen Sie **Neu** aus.

- Geben Sie als Namen der Richtlinie **Nessus Scan GPO** ein.

Schritt 3: Richtlinie konfigurieren, um die Gruppe „Nessus Local Access“ als Administratoren festzulegen
Hier fügen Sie der Richtlinie **Nessus Scan GPO** die Gruppe **Nessus Local Access** hinzu und legen sie in den Gruppen ab, die diese Richtlinie verwenden.

- Klicken Sie auf die Richtlinie **Nessus Scan GPO** und wählen Sie dann **Bearbeiten** aus.
- Blenden Sie ***Computerkonfiguration\Richtlinien\Windows-Einstellungen\Sicherheitseinstellungen\Eingeschränkte Gruppen*** ein.
- Klicken Sie im linken Bereich mit der rechten Maustaste auf **Eingeschränkte Gruppen** und wählen Sie „**Gruppe hinzufügen**“ aus.
- Wählen Sie „**Durchsuchen**“ im Dialogfeld **Gruppe hinzufügen** aus, geben Sie **Nessus Local Access** ein und klicken Sie dann auf **Namen überprüfen**.
- Klicken Sie zwei Mal auf **OK**, um das Dialogfeld zu schließen.
- Klicken Sie unter ***Diese Gruppe ist Mitglied von:*** auf „**Hinzufügen**“.
- Fügen Sie die Gruppe „*Administratoren*“ hinzu.
- Klicken Sie zwei Mal auf **OK**.

Schritt 4: Sicherstellen, dass die betreffenden Ports für die Nessus-Verbindung mit dem Host in der Firewall geöffnet sind
Nessus verwendet SMB (Server Message Block) und WMI (Windows-Verwaltungsinstrumentation), weswegen der Zugriff auf das System durch die Windows-Firewall zugelassen werden muss.

WMI über die Windows XP- und Windows 2003-Firewall zulassen
- Klicken Sie auf die Richtlinie **Nessus Scan GPO** und wählen Sie dann **Bearbeiten** aus.
- Blenden Sie ***Computerkonfiguration\Richtlinien\Administrative Vorlagen\Netzwerk\Netzwerkverbindungen\Windows-Firewall\Domänenprofil*** *ein*.
    - ***Hinweis***: Der Hauptgrund für die Konfiguration des Domänenprofils anstelle des Standardprofils besteht darin, dass das Domänenprofil nur dann angewendet wird, wenn Windows eine Verbindung mit einem Netzwerk erkennt, das Teil der ihm zugehörigen Domäne ist. Das Standardprofil wird angewendet, wenn die Hosts nicht feststellen können, ob die Anfrage aus einem Netzwerkbereich einer Domäne oder einem öffentlichen Netzwerk stammt; hierdurch werden Risiken für den unautorisierten Zugriff auf WMI-Ports verringert.
- Wählen Sie **Windows-Firewall: Eingehende Programmausnahmen festlegen**. Klicken Sie dann mit der rechten Maustaste und wählen Sie **Bearbeiten** aus dem Kontextmenü aus (alternativ doppelklicken Sie auf den Eintrag).
    - Wählen Sie **Aktiviert** aus.
    - Klicken Sie auf **Anzeigen**.
    - Geben Sie in den Definitionen für die **Programmausnahmen** Folgendes ein:
        - %windir%\system32\wbem\unsecapp.exe:*:enable:wmi
        - %windir%\system32\dllhost.exe:*:enable:ddlhost
        - ***Hinweis***: In den oben genannten Einträgen steht * für den Platzhalter, damit sich beliebige IP-Adressen in der Domäne mit diesen Diensten verbinden können. Sie können die Sicherheit steigern, indem Sie nur bestimmte IP-Adressen oder -Adressbereiche, bei denen Verwaltungstools die Verbindung mit dem Port herstellen, oder die IP-Adresse des Nessus-Scanners zulassen.
    - Klicken Sie auf **OK**.
    - Klicken Sie auf **OK**, um die Liste der Richtlinien für die Firewall aufzurufen.

- Wählen Sie **Windows-Firewall: Ausnahmen für lokale Ports zulassen** aus, klicken Sie mit der rechten Maustaste und wählen Sie **Bearbeiten** aus dem Kontextmenü aus (alternativ doppelklicken Sie auf den Eintrag).
  - Wählen Sie **Aktiviert (Aktiviert)**aus.
  - Klicken Sie auf **OK**.
- Wählen Sie **Windows-Firewall: Eingehende Programmausnahmen festlegen** aus, klicken Sie mit der rechten Maustaste und wählen Sie **Bearbeiten** aus dem Kontextmenü aus (alternativ doppelklicken Sie auf den Eintrag).
  - Wählen Sie **Aktiviert** aus.
  - Klicken Sie auf **Anzeigen**.
  - Geben Sie in den Definitionen für die **Portausnahmen** Folgendes ein:
    - 135:TCP:*:enable
    - ***Hinweis***: In den oben genannten Einträgen steht * für den Platzhalter, damit sich beliebige IP-Adressen in der Domäne mit diesen Diensten verbinden können. Sie können die Sicherheit steigern, indem Sie nur bestimmte IP-Adressen oder -Adressbereiche, bei denen Verwaltungstools die Verbindung mit dem Port herstellen, oder die IP-Adresse des Nessus-Scanners zulassen.
  - Klicken Sie auf **OK**, um die Liste der Firewall-Richtlinien aufzurufen.
- Wählen Sie **Windows-Firewall: Eingehende Portausnahmen festlegen** aus, klicken Sie mit der rechten Maustaste und wählen Sie **Bearbeiten** aus dem Kontextmenü aus (alternativ doppelklicken Sie auf den Eintrag).
  - Wählen Sie **Aktiviert** aus.
  - Klicken Sie auf das Feld **Unerbetene eingehende Meldungen von diesen IP-Adressen zulassen** und geben Sie * ein.
  - ***Hinweis***: In den oben genannten Einträgen steht * für den Platzhalter, damit sich beliebige IP-Adressen in der Domäne mit diesen Diensten verbinden können. Sie können die Sicherheit steigern, indem Sie nur bestimmte IP-Adressen oder -Adressbereiche, bei denen Verwaltungstools die Verbindung mit dem Port herstellen, oder die IP-Adresse des Nessus-Scanners zulassen.
  - Klicken Sie auf **OK**, um die Firewall-Richtlinien aufzurufen.

WMI über Windows Vista-, 7-, 8-, 2008-, 2008R2- und 2012-Firewall zulassen

- Klicken Sie auf die Richtlinie **Nessus Scan GPO** und wählen Sie **Bearbeiten** aus.
- Blenden Sie ***Computerkonfiguration\Richtlinien\Windows-Einstellungen\Windows-Firewall mit erweiterter Sicherheit\Windows-Firewall mit erweiterter Sicherheit\Eingehende Regeln*** *ein.*
- Klicken Sie mit der rechten Maustaste in den Arbeitsbereich und wählen Sie **Neue Regel** aus.
- Markieren Sie die Option **Vordefiniert** und wählen Sie **Windows-Verwaltungsinstrumentation (WMI)** aus der Dropdownliste.
- Klicken Sie auf **Weiter**.
- Aktivieren Sie die folgenden Kontrollkästchen:
  - Windows-Verwaltungsinstrumentation (ASync eingehend)
  - Windows-Verwaltungsinstrumentation (WMI eingehend)

- Windows-Verwaltungsinstrumentation (DCOM eingehend)

- Klicken Sie auf **Weiter**.
- Klicken Sie auf **Fertig stellen**.
- ***Hinweis***: Vordefinierte Richtlinien können später bearbeitet werden, um Verbindungen mit den Ports basierend auf IP-Adresse und Domänenbenutzer einzuschränken und so das Risiko eines Missbrauchs von WMI zu senken.

Schritt 5: Gruppenrichtlinienobjekt verknüpfen

- Klicken Sie in der Gruppenrichtlinien-Verwaltungskonsole mit der rechten Maustaste auf die Domäne oder Organisationseinheit und wählen Sie **Vorhandenes Gruppenrichtlinienobjekt verknüpfen** aus.
- Wählen Sie das Gruppenrichtlinienobjekt „Nessus Scan GPO“ aus.

Windows XP und Windows 2003 konfigurieren

Für die Durchführung authentifizierter Scans auf Windows XP- oder Windows 2003-Systemen müssen verschiedene Konfigurationsoptionen aktiviert werden:

1. Der WMI-Dienst muss auf dem Zielsystem aktiviert sein.
2. Der Dienst „Remote-Registrierung“ muss aktiviert sein (standardmäßig ist er deaktiviert). Er kann entweder vom Administrator oder durch Nessus für fortlaufende Audits manuell aktiviert werden. Mit den Plugins 42897 und 42898 kann Nessus den Dienst auf die Dauer des Scans beschränken.
3. Die Datei- und Druckerfreigabe muss in der Netzwerkkonfiguration des Zielsystems aktiviert sein.
4. Zwischen dem Nessus-Scanner und dem Zielsystem müssen die Ports 139 und 445 offen sein.
5. Es muss ein SMB-Konto verwendet werden, das auf dem Zielsystem über lokale Administratorrechte verfügt.

Unter Umständen müssen Sie die lokalen Windows-Sicherheitsrichtlinien ändern, da andernfalls der Zugriff oder geerbte Berechtigungen gesperrt werden könnten. Eine Richtlinie, die authentifizierte Scans häufig beeinträchtigt, finden Sie unter:

Verwaltung > Lokale Sicherheitsrichtlinie > Sicherheitseinstellungen > Lokale Richtlinien > Sicherheitsoptionen > Netzwerkzugriff: Modell zur gemeinsamen Nutzung und Sicherheitsmodell für lokale Konten

Wenn diese lokale Sicherheitsrichtlinie einen anderen Wert als „Klassisch - lokale Benutzer authentifizieren sich als sie selbst“ hat, kann ein Compliancetest nicht erfolgreich ausgeführt werden.

Windows 2008, Windows Vista und Windows 7 konfigurieren

Für die Durchführung authentifizierter Scans auf Windows 2008-, Windows Vista- oder Windows 7-Systemen müssen verschiedene Konfigurationsoptionen aktiviert werden:

1. Unter „Windows-Firewall“ > „Windows-Firewalleinstellungen“ muss die Option „Datei- und Druckerfreigabe“ aktiviert werden.
2. Rufen Sie über das Tool `gpedit.msc` (das Sie über „Ausführen...“ starten) den Gruppenrichtlinienobjekt-Editor auf. Navigieren Sie zu „Richtlinie für Lokaler Computer“ > „Administrative Vorlagen“ > „Netzwerk“ > „Netzwerkverbindungen“ > „Windows-Firewall“ > „Standardprofil“ > „Windows-Firewall: Eingehende Ausnahme für Datei- und Druckerfreigabe zulassen“ und aktivieren Sie die Richtlinie.
3. Im Gruppenrichtlinienobjekt-Editor muss „Lokale Computerrichtlinie“ > „Administrative Vorlagen“ > „Netzwerk“ > „Netzwerkverbindungen“ > „Verwendung des Internetverbindungsfirewalls im eigenen DNS-Domänennetzwerk nicht zulassen“ auf „Deaktiviert“ oder „Nicht konfiguriert“ gesetzt sein.

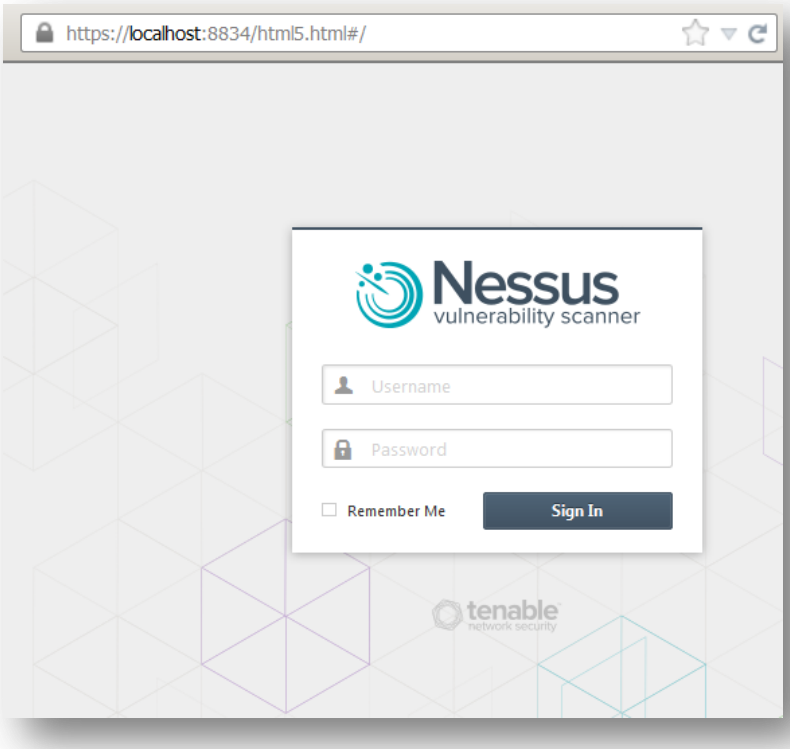
4. Der Dienst „Remote-Registrierung“ muss aktiviert sein (standardmäßig ist er deaktiviert). Er kann entweder vom Administrator oder durch Nessus für fortlaufende Audits manuell aktiviert werden. Mit den Plugins 42897 und 42898 kann Nessus den Dienst auf die Dauer des Scans beschränken.

Nessus kann den Dienst „Remote-Registrierung“ aktivieren und deaktivieren. Zu diesem Zweck muss auf dem Zielsystem die Einstellung „Manuell“ anstelle von „Deaktiviert“ für den Dienst „Remote-Registrierung“ konfiguriert sein.

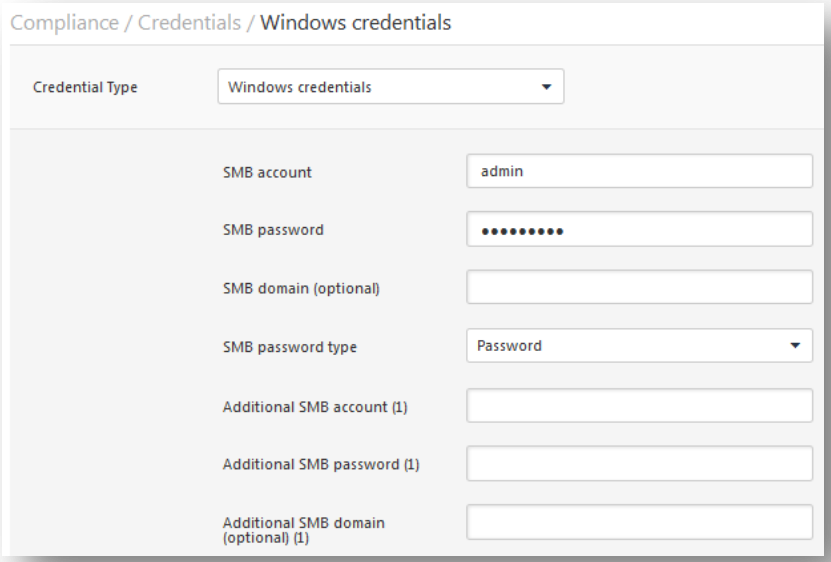
Die Windows-Benutzerkontensteuerung (UAC) kann auch deaktiviert werden, was jedoch nicht empfohlen wird. Öffnen Sie zum vollständigen Abschalten der Benutzerkontensteuerung die Systemsteuerung, wählen Sie „Benutzerkonten“ aus und deaktivieren Sie die Option „Benutzerkontensteuerung ein- oder ausschalten“. Alternativ können Sie auch einen neuen Registrierungsschlüssel namens „LocalAccountTokenFilterPolicy“ erstellen und dessen Wert auf „1“ setzen. Dieser Schlüssel muss in der Registrierung an folgender Stelle eingerichtet werden: **`HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system\LocalAccountTokenFilterPolicy`**. Weitere Informationen zu dieser Registrierungseinstellung entnehmen Sie folgendem Artikel: MSDN 766945 KB.

Nessus für Windows-Anmeldungen konfigurieren

Die Nessus-Benutzeroberfläche



Öffnen Sie einen Webbrowser, stellen Sie wie oben gezeigt eine Verbindung mit der Benutzeroberfläche des Nessus-Scanners her und klicken Sie auf die Registerkarte „Policies“ („Richtlinien“). Erstellen Sie eine neue oder bearbeiten Sie eine vorhandene Richtlinie und wählen Sie dann die Registerkarte „Credentials“ („Anmeldedaten“) auf der linken Seite aus. Wählen Sie „Windows credentials“ („Windows-Anmeldedaten“) aus dem Dropdownmenü oben im Fenster aus:



Geben Sie den SMB-Kontennamen, das Kennwort und optional die Domäne an.

Klicken Sie unten im Fenster auf „**Submit**“ („Senden“), um die Konfiguration abzuschließen. Die neue Scanrichtlinie wird nun der Liste der verwalteten Scanrichtlinien hinzugefügt.

Nessus-Befehlszeile für UNIX

.nessus-Dateien verwenden

Nessus kann konfigurierte Scanrichtlinien, Netzwerkziele und Berichte als `.nessus`-Datei speichern. Die Erstellung einer `.nessus`-Datei, die Windows-Anmeldedaten enthält, ist weiter oben im Abschnitt „Nessus User Guide“ („Die Nessus-Benutzeroberfläche“) beschrieben. Hinweise zur Ausführung eines Befehlszeilenscans mithilfe der `.nessus`-Datei entnehmen Sie dem Nessus-Benutzerhandbuch. Dieses ist verfügbar unter:

http://www.tenable.com/products/nessus/documentation

.nessusrc-Dateien verwenden

Wenn Sie eine `.nessusrc`-Datei manuell erstellen, ermöglichen drei Einträge wie nachfolgend gezeigt die Konfiguration von Benutzername, Kennwort und optionaler Domäne:

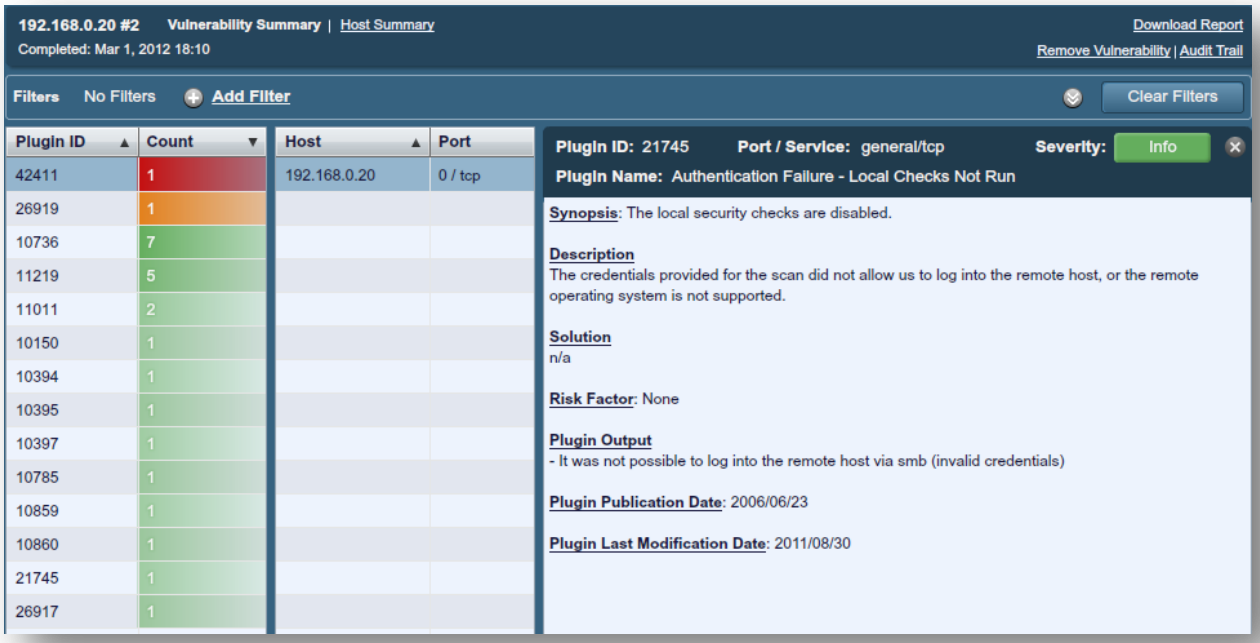
```
Login configurations[entry]:SMB account : =
Login configurations[password]:SMB password : =
Login configurations[entry]:SMB domain (optional) : =
```

Fehlerhafte Anmeldedaten erkennen

Wenn Sie Nessus zur Durchführung authentifizierter Audits von UNIX- oder Windows-Systemen verwenden, kann die Feststellung, ob Sie korrekte Kennwörter und SSH-Schlüssel verwendet haben, anhand einer Analyse der Ergebnisse schwierig sein. Allerdings können Nessus-Benutzer nun ganz einfach feststellen, ob ihre Anmeldedaten funktionieren oder nicht. Zu diesem Zweck hat Tenable der Plugin-Familie „Settings“ das Nessus-Plugin 21745 hinzugefügt.

Mit diesem Plugin kann festgestellt werden, ob das Anmelden am Remotehost für den Scan aufgrund ungeeigneter Windows- oder SSH-Anmeldedaten nicht möglich war. War die Anmeldung erfolgreich, dann gibt dieses Plugin kein

Ergebnis aus. Nachfolgend gezeigt ist ein Berichtsbeispiel, das bei dem Versuch generiert wurde, sich mit Nessus unter Verwendung eines falschen Benutzernamens oder Kennworts an einem Remotecomputer anzumelden:


192.168.0.20 #2 Vulnerability Summary | Host Summary
Completed: Mar 1, 2012 18:10
Download Report
Remove Vulnerability | Audit Trail
Filters No Filters Add Filter
Clear Filters
Plugin ID Count
42411 1
26919 1
10736 7
11219 5
11011 2
10150 1
10394 1
10395 1
10397 1
10785 1
10859 1
10860 1
21745 1
26917 1
Host Port
192.168.0.20 0 / tcp
Plugin ID: 21745 Port / Service: general/tcp Severity: Info
Plugin Name: Authentication Failure - Local Checks Not Run
Synopsis: The local security checks are disabled.
Description
The credentials provided for the scan did not allow us to log into the remote host, or the remote operating system is not supported.
Solution
n/a
Risk Factor: None
Plugin Output
- It was not possible to log into the remote host via smb (invalid credentials)
Plugin Publication Date: 2006/06/23
Plugin Last Modification Date: 2011/08/30

Problembehebung

F.: Wie erkenne ich, ob der lokale Scan funktioniert?

A.: Sofern auf ihrem Server nicht 100 Prozent aller erforderlichen Patches vorhanden sind, wird ein lokaler Scan als Ergebnis wahrscheinlich Informationen zu Patches ausgeben. Ferner wird je nach Betriebssystem eine Anzahl von Auditinformationen zurückgegeben.

Es kann auch nützlich sein, Nessus aus der Analyse herauszunehmen und dann zu testen, ob die Konten und Netzwerke richtig konfiguriert sind. Führen Sie unter Verwendung des einfachen UNIX-Befehls „**`id`**“ vom Nessus-Scanner aus den folgenden Befehl aus:

```
# ssh -i /home/test/nessus/ssh_key nessus@192.1.1.44 id
#
```

Vergewissern Sie sich, dass Sie die IP-Adresse des Systems, mit dem die Vertrauensbeziehung konfiguriert wurde, sowie das richtige Benutzerkonto verwenden (in diesem Falle „nessus“). War der Befehl erfolgreich, dann sehen Sie die Ergebnisse des **`id`**-Befehls so, als wäre dieser auf Ihrem Remotesystem ausgeführt worden.

Bei UNIX-Audits meldet das Skript **`ssh_get_info.nasl`**, ob die Authentifizierung erfolgreich war. Falls die SSH-Anmeldung nicht funktioniert, können Sie die Einstellung „report_verbosity“ für Ihren Nessus-Scan auf „Verbose“ („Ausführlich“) setzen. Auf diese Weise werden alle Fehler- und Diagnosemeldungen angezeigt, solange das betreffende Skript ausgeführt wird.

Bei Windows-Audits geben die Skripts **`smb_login.nasl`** und **`smb_registry_access.nasl`** an, ob der während des Scans angegebene Benutzername und das Kennwort korrekt waren und ob die Remote-Registrierung gelesen werden konnte. Das Skript **`smb_registry_full_access.nasl`** gibt nur dann eine Warnung aus, wenn die Registrierung nicht

vollständig gelesen werden konnte. Den Ergebnissen hostbasierter Tests für Audits eines Windows-Servers können Sie entnehmen, ob die Anmeldedaten funktioniert haben.

Außerdem kann mit dem Skript **`hostlevel_check_failed.nasl`** festgestellt werden, ob das Anmelden am Remotehost für einen Scan aufgrund ungeeigneter Windows- oder SSH-Anmeldedaten nicht möglich war.

F.: Wie erkenne ich, wenn der lokale Scan nicht funktioniert?

A.: Auf Windows-Systemen werden in diesem Fall Anmeldefehlerereignisse auf dem Server generiert. Falls ein Domänencontroller verwendet wird, sind auch dort Anmeldefehlerereignisse zu finden.

Auf UNIX-Systemen werden Anmeldefehler in den Systemlogdateien (z. B. „**`/var/log/messages`**“) aufgeführt, sofern kein Kerberos-Remotecontroller verwendet wird.

Außerdem kann mit dem Skript **`hostlevel_check_failed.nasl`** festgestellt werden, ob das Anmelden am Remotehost für einen Scan aufgrund ungeeigneter Windows- oder SSH-Anmeldedaten nicht möglich war.

F.: Welche Probleme können bei Hosttests noch auftreten?

A.: Es gibt eine ganze Reihe von Faktoren, die den Zugriff unterbinden können. Hierzu gehören etwa die Folgenden:

- Netzwerkfirewalls, die Port 22 für SSH unter UNIX oder Port 445 unter Windows filtern
- Hostbasierte Firewalls, die Verbindungen über die genannten Ports unterbinden
- Administratoren, die auf UNIX-Systemen SSH auf einen anderen Port als 22 verschieben
- Einige host- und netzwerkbasierte Intrusion-Prevention-Systeme, die den Remotezugriff verhindern
- Gescannte Systeme, die weder ein UNIX- noch ein Windows-Server sind und stattdessen ein Drucker, ein Router, ein Faxgerät oder ein Anzeigegerät sein könnten

F.: Ich teste SSH-Verbindungen vom Shell-Prompt der Scanzielhosts zum Nessus-System, um die Konnektivität zu überprüfen. Bei der Verbindung kommt es zu Verzögerungen. Wieso ist das so?

A.: Ursache hierfür ist höchstwahrscheinlich ein infolge einer DNS-Fehlkonfiguration durchgeführter DNS-Lookup. Wenn Ihre Site DNS verwendet, wenden Sie sich an Ihren DNS-Administrator, um die Konfigurationsprobleme beheben zu lassen. Eine mögliche Ursache könnten fehlende Reverse-Lookup-Zonen sein. Gehen Sie zum Testen von DNS-Lookups wie folgt vor:

```
# host IP_ADRR_OF_NESSUS_SERVER
```

Wenn Sie „dig“ installiert haben, können Sie die Überprüfung auch wie folgt durchführen:

```
# dig -x IP_ADRR_OF_NESSUS_SERVER
```

Verwendet Ihre Site DNS nicht, dann können Sie die nachfolgend beschriebenen Schritte ausführen, um die Ausführung von DNS-Lookups zu übergehen.

1. Bearbeiten Sie die Datei **`/etc/nsswitch.conf`** so, dass die Zeile „hosts:“ den Wert „hosts: files“ erhält. Hinweis: Bei manchen OpenSSH-Versionen ist dieser Schritt unter Umständen ungültig.

2. Fügen Sie der Datei **`/etc/hosts`** auf dem System die IP-Adresse/den Namen des Servers, auf dem Nessus ausgeführt wird, hinzu.

3. Konfigurieren Sie den OpenSSH-Remoteserver so, dass DNS-Lookups auf einem Host **nicht** ausgeführt werden. Hierzu nehmen Sie folgende Einstellungen vor:

   - „UseDNS no“ in der Datei **`sshd_config`** (für Release 3.8; der Standardwert ist „yes“)

   - „VerifyReverseMapping no“

Wie Sie Ihren Scanner schützen

Warum sollte ich meinen Scanner schützen?

Wenn Sie den Nessus-Scanner für die Verwendung von Anmeldedaten auf einem UNIX- oder Windows-Server konfigurieren, verfügt Ihr System über Anmeldedaten, die von einem Angreifer missbraucht werden könnten. Um dies zu verhindern, müssen Sie nicht nur gut auf die Sicherheit des Betriebssystems achten, unter dem Ihr Scanner ausgeführt wird, sondern sich auch darüber im Klaren sein, dass es für Angreifer Mittel und Wege geben könnte, den Scanner zur Preisgabe von Sicherheitsinformationen zu bewegen.

Wie schottet man einen Scanner ab?

Im Idealfall würde der Nessus-Scanner vollständig über eine Systemkonsole angesteuert werden und keine Netzwerkverbindungen von Remotehosts annehmen. Ein solches System müsste physisch so abgesichert sein, dass nur Berechtigte darauf zugreifen könnten. Ein solcher Server könnte durch eine externe Firewall oder einen Switch, mit dem Scans auf bestimmte Netzwerke beschränkt werden könnten, weiter abgeschottet werden. Sie dürfen Personal-Firewall-Software allerdings nicht direkt auf dem Nessus-Scannersystem installieren. Denken Sie auch daran, dass Nessus auf das Scannen bestimmter Netzwerke beschränkt werden kann.

Ein solcher Scanner wäre nicht allzu nützlich. Ziehen Sie in Betracht, einen Remotenetzwerkzugriff auf den Server zuzulassen. Nessus unterstützt standardmäßig HTTP-Verbindungen über Port 8834. Eine Systemfirewall kann so konfiguriert werden, dass nur Verbindungen gültiger Nessus-Clients angenommen werden, die über Port 8834 eingehen.

Wenn das System remote administriert oder bedient werden soll, kann auch ein sicherer Remotezugriff verwendet werden. Unter UNIX lässt sich hierfür das SSH-Protokoll (Secure Shell) verwenden. Halten Sie den SSH-Daemon auf dem aktuellen Stand, und verwenden Sie starke Kennwörter und/oder noch stärkere Authentifizierungsmethoden. Auf Windows-Servern bieten die Terminaldienste ein ausreichendes Maß an Kontrolle über die Dienste für Nessus Windows. In beiden Fällen sollten Sie das System immer so aktuell wie möglich halten und keine nicht erforderlichen Netzwerkdienste ausführen. Anleitungen zum Härten von Systemen entnehmen Sie den CIS-Benchmarks (Center for Internet Security).

Sichere Implementierung von SSH-Audits unter UNIX

Verwenden Sie niemals SSH-Kennwörter zur Durchführung von Remotescans. Wenn Sie ein Netzwerk scannen, müsste ein böswilliger Benutzer lediglich einen modifizierten SSH-Daemon ausführen und die Eingaben für Benutzername und Kennwort aufzeichnen. Auch wenn Sie für jeden Host eine eindeutige Kombination aus Benutzername und Kennwort verwenden, ist die Verwendung statischer Kennwörter risikobehaftet.

Wenn Sie sich über ein gefährdetes System mit einem Kennwort an einem Server anmelden, besteht die Chance, dass das Kennwort entwendet wird, da es über eine SSH-Verbindung gesendet wird. Nachdem der Angreifer den Remoteserver übernommen hat, kann er den SSH-Daemon durch einen eigenen ersetzen, der die Kennwörter eingehender Verbindungen protokolliert.

Sichere Windows-Audits

Wenn die Option „Only use NTLMv2“ („Nur NTLMv2 verwenden“) deaktiviert wurde, ist es theoretisch möglich, Nessus unter Verwendung von Version 1 des NTLM-Protokolls zu einer Anmeldung an einem Windows-Server mit Domänenanmeldedaten zu bewegen. Dies bietet einem Remote-Angreifer die Möglichkeit, einen bei Nessus abgerufenen Hashwert zu verwenden. Dieser Hashwert kann möglicherweise geknackt werden, um so einen Benutzernamen oder ein Kennwort zu erschließen. Außerdem ermöglicht er unter Umständen auch eine direkte Anmeldung bei anderen Servern. Erzwingen Sie die Verwendung von NTLMv2 durch Nessus, indem Sie die Scaneinstellung „Only use NTLMv2“ vor

Beginn des Scans aktivieren. Auf diese Weise wird verhindert, dass der Windows-Server eines Angreifers mithilfe von NTLM an einen Hashwert gelangen kann.

Bei NTLMv2 kann die SMB-Signierung verwendet werden. Stellen Sie sicher, dass die SMB-Signierung auf allen Ihren Windows-Servern aktiviert ist, denn nur so kann verhindert werden, dass ein Server einen Hashwert aus einem Nessus-Scan abrufen und diesen wiederverwenden kann. Außerdem müssen Sie mit einer Richtlinie die Verwendung starker Kennwörter erzwingen, die mithilfe von Wörterbuchattacken wie John the Ripper und L0phtCrack nicht so einfach geknackt werden können.

Beachten Sie, dass es eine Unmenge unterschiedlicher Angriffsformen gegen die Windows-Sicherheit gibt, mit denen Hashwerte abgegriffen werden sollen, die dann für Angriffe wiederverwendet werden können. Mit der SMB-Signierung verbessern Sie den Schutz gegen derartige Man-in-the-Middle-Angriffe.

Weitere Informationen

Tenable hat eine Reihe von Dokumenten erstellt, in denen die Bereitstellung, Installation, Konfiguration, der Betrieb und die Testmethoden von Nessus ausführlich beschrieben werden:

- **Nessus 5.2 Installation and Configuration Guide** („Nessus 5.2-Installations- und Konfigurationshandbuch“; Schrittanleitung zur Nessus-Installation und -Konfiguration)
- **Nessus 5.2 User Guide** („Nessus 5.2-Benutzerhandbuch“; beschreibt den Einsatz des Nessus Nessus-Sicherheitslückenscanners einschließlich Konfiguration und Berichterstellung)
- **Nessus 5.2-Benutzerhandbuch** (beschreibt Konfiguration und Bedienung der Nessus-Benutzeroberfläche)
- **Nessus Compliance Checks** („Nessus-Compliancetests“; allgemeiner Leitfaden zum Verständnis und zur Durchführung von Compliancetests mithilfe von Nessus und SecurityCenter)
- **Nessus Compliance Checks Reference** („Nessus-Referenzhandbuch für Compliancetests“; umfassender Leitfaden zur Syntax von Nessus-Compliancetests)
- **Nessus v2 File Format** („Nessus V2-Dateiformat“; beschreibt die Struktur des `.nessus`-Dateiformats, das mit Nessus 3.2 und NessusClient 3.2 eingeführt wurde)
- **Nessus 5.0 REST Protocol Specification** („Nessus 5.0 REST-Protokollspezifikation“; beschreibt das REST-Protokoll und die Schnittstelle in Nessus)
- **Nessus 5 and Antivirus** („Nessus 5 und Virenschutz“; beschreibt die Funktion verschiedener gängiger Sicherheitssoftwarepakete in Nessus und enthält Tipps und Lösungsvorschläge für eine verbesserte Funktionsweise der Software ohne Einschränkung der Sicherheit oder Verhinderung Ihrer Sicherheitslückenscans)
- **Nessus 5 and Mobile Device Scanning** („Nessus 5 und Scans von Mobilgeräten“; beschreibt die Integration von Nessus in Microsoft Active Directory und Verwaltungsserver für Mobilgeräte zur Bestimmung von im Netzwerk eingesetzten Mobilgeräten)
- **Nessus 5.0 and Scanning Virtual Machines** („Nessus 5.0 und Scans virtueller Maschinen“; beschreibt den Einsatz des Sicherheitslückenscanners von Tenable Network Security Nessus für Audits der Konfiguration virtueller Plattformen sowie der darauf ausgeführten Software)
- **Strategic Anti-malware Monitoring with Nessus, PVS, and LCE** („Strategische Malwareüberwachung mit Nessus, PVS und LCE“; beschreibt, wie mithilfe der Tenable USM-Plattform zahlreiche bösartige Softwareprogramme erkannt werden können und das Ausmaß der Malware-Infizierung bestimmt werden kann)

- **Patch Management Integration** („Integration des Patchmanagements“; beschreibt, wie Nessus und SecurityCenter mithilfe von Berechtigungen auf die IBM TEM-, Microsoft WSUS- und SCCM-, VMware Go- und Red Hat Network Satellite-Patchmanagementsysteme Patch-Audits auf Systemen ausführen, für die dem Nessus-Scanner möglicherweise keine Berechtigungen zur Verfügung stehen)
- **Real-Time Compliance Monitoring** („Compliance-Überwachung in Echtzeit“; erläutert, wie die Lösungen von Tenable Sie bei der Erfüllung zahlreicher gesetzlicher Vorschriften und Finanzstandards unterstützen)
- **Tenable Products Plugin Families** („Tenable Produkt-Plugin-Familien“; stellt eine Beschreibung und Zusammenfassung der Plugin-Serien für Nessus, Log Correlation Engine und den Passive Vulnerability Scanner bereit)
- **SecurityCenter Administration Guide** („SecurityCenter-Administratorhandbuch“)

Weitere Onlineressourcen sind nachfolgend aufgeführt:

- Nessus-Diskussionsforum: https://discussions.nessus.org/
- Tenable-Blog: http://www.tenable.com/blog
- Tenable-Podcast: http://www.tenable.com/podcast
- Beispielvideos zum Gebrauch: http://www.youtube.com/user/tenablesecurity
- Tenable-Twitterfeed: http://twitter.com/tenablesecurity

Setzen Sie sich mit uns in Verbindung – via E-Mail (support@tenable.com, sales@tenable.com) oder über unsere Website unter http://www.tenable.com/.

Wissenswertes zu Tenable Network Security

Wenn es um die frühzeitige Erkennung neu entwickelter Sicherheitslücken, Bedrohungen und Compliance-relevanter Risiken geht, verlassen sich mehr als 20.000 Organisationen auf Tenable Network Security. Hierzu gehören neben dem gesamten US-Verteidigungsministerium eine Reihe von Großunternehmen und Regierungsbehörden weltweit. Die Nessus- und SecurityCenter-Lösungen sind nach wie vor branchenführend beim Ermitteln von Sicherheitslücken, beim Verhindern von Angriffen und bei der Erfüllung einer Vielzahl gesetzlicher Vorschriften. Weitere Informationen finden Sie unter www.tenable.com.

GLOBALE UNTERNEHMENSZENTRALE

Tenable Network Security
7021 Columbia Gateway Drive
Suite 500
Columbia, MD 21046, USA
+1.410.872.0555
www.tenable.com

Copyright © 2014. Tenable Network Security, Inc. Alle Rechte vorbehalten. Tenable Network Security und Nessus sind eingetragene Marken von Tenable Network Security, Inc.